UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I - CAMPINA GRANDE
CENTRO CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

FLÁVIA MARIA DE BRITO SANTOS

UM ESTUDO DO TEOREMA DE LAGRANGE E SUAS APLICAÇÕES

CAMPINA GRANDE
2024

FLÁVIA MARIA DE BRITO SANTOS

UM ESTUDO DO TEOREMA DE LAGRANGE E SUAS APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologias da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciado(a) em Matemática.

Área de concentração: Matemática pura

Orientador: Prof. Dr. José Lucas Galdino da Silva

CAMPINA GRANDE
2024

S237s Santos, Flavia Maria de Brito.
Um estudo do teorema de lagrange e suas aplicações [manuscrito] / Flavia Maria de Brito Santos. - 2024.
39 f. : il.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2024.

"Orientação : Prof. Dr. José Lucas Galdino da Silva, Departamento de Matemática - CCT".

1. Estruturas algébricas. 2. Teoria de Grupos. 3. Teorema de Lagrange. I. Título

21. ed. CDD 510

Elaborada por Bruno Rafael Freitas de Lima - CRB - 15/1021 BC

FLÁVIA MARIA DE BRITO SANTOS

UM ESTUDO DO TEOREMA DE LAGRANGE E SUAS APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologias da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Licenciado(a) em Matemática.

Área de concentração: Matemática pura

Aprovada em: 19/11/2024.

Documento assinado eletronicamente por:

- **Emanuela Régia de Sousa Coelho** (***.622.214-**), em **28/11/2024 06:15:27** com chave **4ec6e2bead6911ef8c541a1c3150b54b**.
- **Matheus Marques de Araújo** (***.259.704-**), em **27/11/2024 23:33:58** com chave **38b2ed16ad3111efae081a1c3150b54b**.
- **José Lucas Galdino da Silva** (***.857.714-**), em **27/11/2024 23:17:44** com chave **f40656f0ad2e11efae5606adb0a3afce**.

Documento emitido pelo SUAP. Para comprovar sua autenticidade, faça a leitura do QrCode ao lado ou acesse https://suap.uepb.edu.br/comum/autenticar_documento/ e informe os dados a seguir.
Tipo de Documento: Termo de Aprovação de Projeto Final
Data da Emissão: 28/11/2024
Código de Autenticação: dff730

Dedico à minha família, pelo amor e apoio prestado.

AGRADECIMENTOS

Primeiramente, agradeço a Deus, que sempre me guiou e me deu força em cada passo dessa jornada. Agradeço à minha família, em especial à minha cunhada Wezila e ao meu irmão Ricardo, por toda a motivação e suporte incondicional ao longo da minha trajetória. Agradeço também ao meu orientador, cuja paciência e dedicação foram fundamentais para a conclusão deste trabalho. Sem sua ajuda, nada diso teria sido possível. Por fim, agradeço aos meus amigos Thayná, Vanessa, Isaac, Israel, Ingrid, Gabriel, Igor, Ednaldo, Jacqueline, Vitória, Anderson e Joane, que sempre trouxeram o melhor de mim e incentivaram a seguir meus objetivos.

Meu muito obrigada a todos!

“Aprender é a única coisa de que a mente nunca se cansa, nunca tem medo e nunca se arrepende.” (Leonardo da Vinci)

RESUMO

Este trabalho apresenta o Teorema de Lagrange, um dos resultados fundamentais na teoria de grupos finitos. Foi realizada uma pesquisa de cunho bibliográfico a fim de apresentar alguns tópicos importantes deste trabalho. Inicia-se com uma breve introdução ao tema, seguida pela exposição dos conceitos essenciais da Teoria dos Grupos, com exemplos e resultados relevantes que fundamentam o estudo subsequente. Em seguida, é apresentada a demonstração do Teorema de Lagrange, acompanhada de algumas de suas aplicações no contexto dos grupos finitos. O objetivo é oferecer suporte didático para estudantes de graduação, especialmente aqueles do curso de Licenciatura em Matemática, reforçando os conceitos abordados na disciplina de Estruturas Algébricas.

Palavras-chave: estruturas algébricas; teoria de grupos; teorema de Lagrange.

ABSTRACT

This work presents Lagrange's Theorem, one of the fundamental results in finite group theory. A bibliographical research was carried out in order to present some important topics of this work. It begins with a brief introduction to the topic, followed by the exposition of the essential concepts of Group Theory, with examples and relevant results that support the subsequent study. Next, the demonstration of Lagrange's Theorem is presented, accompanied by some of its applications in the context of finite groups. The objective is to offer teaching support for undergraduate students, especially those on the Mathematics Degree course, reinforcing the concepts covered in the Algebraic Structures discipline.

Keywords: algebraic structures; group theory; Lagrange's theorem.

SUMÁRIO

Página

1 INTRODUÇÃO

A teoria de grupos é um ramo fundamental da Álgebra Abstrata. Em termos gerais, um grupo é uma coleção de elementos dotada de uma operação binária (como, por exemplo, adição ou multiplicação) que satisfaz quatro propriedades fundamentais: fechamento, associatividade, existência de elemento neutro e existência de inversos. Essas propriedades formam a base que define a estrutura dos grupos e permitem o desenvolvimento de diversas teorias e aplicações. Embora hoje a teoria de grupos seja um campo vasto e profundamente desenvolvido, ela teve suas origens no século XIX, motivada principalmente pelo estudo das simetrias e pela busca de soluções para equações algébricas complexas.

O ponto de partida para a teoria de grupos é geralmente atribuído ao matemático francês Évariste Galois (1811-1832), que fez uma contribuição revolucionária ao estudar as propriedades de permutações e de simetrias. Galois introduziu o conceito de grupo de simetria no contexto de sua pesquisa sobre as soluções de equações polinomiais, formulando a agora chamada teoria de Galois. Esta teoria utiliza grupos para explicar de maneira precisa quando uma equação algébrica pode ou não ser resolvida por radicais, estabelecendo um novo entendimento sobre a relação entre a estrutura das equações e suas soluções. Embora tenha vivido uma vida curta, Galois deixou um legado duradouro e influente, sendo reconhecido como um dos fundadores da teoria dos grupos.

No entanto, o desenvolvimento da teoria de grupos como um campo independente de estudo não foi obra de um único matemático. Na mesma época, outros estudiosos também contribuíram de forma significativa para sua consolidação. Augustin-Louis Cauchy (1789-1857) e Arthur Cayley (1821-1895), por exemplo, desempenharam papéis cruciais . Cauchy introduziu importantes resultados e conceitos sobre grupos de permutações, enquanto Cayley foi o responsável por uma visão mais abstrata dos grupos, formalizando a ideia de grupo como um objeto matemático autônomo, com propriedades que podiam ser estudadas independentemente da natureza de seus elementos específicos. Assim, ao longo do século XIX, a teoria de grupos passou a ser vista como uma área de estudo independente, com um conjunto de ferramentas e métodos próprios que foram se refinando com o tempo.

A teoria de grupos se expandiu rapidamente ao longo dos séculos XIX e XX, tornando-se uma disciplina central dentro da matemática pura e com aplicações em áreas que vão muito além da álgebra abstrata. Na física, a teoria de grupos é fundamental para a compreensão da simetria em sistemas físicos e para a formulação das leis de conservação, essenciais em mecânica quântica. Na química, é usada para descrever simetrias moleculares e as propriedades dos orbitais eletrônicos. Na computação, a teoria de grupos tem aplicações em criptografia e na análise de algoritmos. No campo da criptografia, por exemplo, os conceitos de grupo servem como base para a construção de sistemas de segurança digital, vitais em um mundo cada vez mais interconectado. Dada essa abrangência,

a teoria de grupos não apenas exemplifica a beleza e a coerência interna da matemática, mas também sua aplicabilidade a problemas concretos e interdisciplinares.

Dentro da teoria de grupos, uma classe de grupos é bastante estudada: os grupos finitos. Nesta classe um importante teorema é apresentado, o qual foi formulado por Joseph-Louis Lagrange (1736 - 1813), matemático de destaque cujas contribuições para a matemática influenciaram o desenvolvimento inicial da teoria dos grupos. Embora o conceito de grupo não estivesse totalmente formalizado em sua época, Lagrange contribuiu com ideias que mais tarde seriam vistas como fundamentais para a área. Sua pesquisa em álgebra e teoria dos números impactou muitos dos matemáticos que continuaram a desenvolver a teoria de grupos. Em particular, seu famoso Teorema de Lagrange, formulado em 1770, foi uma contribuição pioneira. Este teorema estabelece que a ordem (ou seja, o número de elementos) de um subgrupo de um grupo finito divide a ordem do grupo inteiro. Essa relação fornece uma ferramenta poderosa para estudar a estrutura dos grupos finitos e é crucial para muitas aplicações posteriores.

Lagrange nasceu em Turim, no Reino da Sardenha (hoje Itália), em uma família de classe média, e mostrou desde cedo uma habilidade excepcional para a matemática. Ao longo de sua carreira, ele trabalhou em áreas como mecânica, onde formulou a mecânica lagrangiana, e em álgebra, onde deixou sua marca com o Teorema de Lagrange. Suas contribuições não apenas ajudaram a solidificar conceitos essenciais na teoria de grupos, mas também prepararam o terreno para a geração de matemáticos que, no século XIX, formalizariam esses conceitos. Embora Lagrange talvez não tenha imaginado o impacto total de suas ideias no campo emergente da teoria dos grupos, seu trabalho lançou bases sólidas para a compreensão das relações entre grupos e seus subgrupos, o que permite hoje a análise da simetria e de transformações em contextos variados. Para a elaboração deste tópico, foram utilizados Eves (2011) e Xavier (2022) como referências para ilustrar o contexto histórico referente a Teoria de Grupos, principais autores e contribuições.

Diante disso, o propósito deste trabalho visa realizar uma pesquisa com abordagem bibliográfica, com base em obras referenciadas pelos seguintes autores: Gonçalves (2015), Iezzi e Domingues (2003), Paixão (2003) e Vieira (2013). Para isso, o trabalho se encontra dividido em dois capítulos principais. No primeiro capítulo, é apresentado os conceitos fundamentais e exemplos de grupos e subgrupos, além da definição de grupos cíclicos. O segundo capítulo aprofunda os tópicos essenciais da teoria, com ênfase nas classes laterais, demonstração detalhada do Teorema de Lagrange e algumas aplicações práticas do Teorema de Lagrange, visando ilustrar sua relevância tanto teórica quanto prática.

2 TEORIA DE GRUPOS

Em muitos sistemas, desde a natureza até os contextos mais abstratos da matemática, existe um conceito recorrente de simetria e organização interna. Esses sistemas possuem elementos que podem ser manipulados ou transformados, mantendo certas propriedades essenciais. Em outras palavras, há uma estrutura que se mantém invariável apesar das operações aplicadas a seus componentes. Por exemplo, ao observar um polígono regular, notamos que ele possui simetrias – rotações e reflexões que o deixam inalterado. Essa ideia de operação que "preserva" certas características é essencial na matemática moderna e está formalizada na teoria dos grupos, um campo que oferece uma estrutura para estudar e classificar esses tipos de simetrias e transformações.

A motivação para estudar grupos surge, portanto, da necessidade de entender e descrever as operações que podem ser aplicadas a um conjunto de elementos sem perder sua estrutura. Essa estrutura de grupo, com suas propriedades específicas, possibilita resolver problemas que vão desde a resolução de equações algébricas até a compreensão de sistemas físicos e químicos.

Neste capítulo além da definição formal de grupo, iremos estudar alguns grupos específicos: subgrupos, grupos cíclicos, o grupo de permutação, entre outros. Tais definições (bem como as suas propriedades) serão utilizadas no próximo capítulo, ao trabalharmos com o Teorema de Lagrange.

2.1 Operações binárias

Antes de trazer o estudo de Grupos, vamos iniciar abordando o conceito e exemplos de operação binária.

Definição 2.1. Seja G um conjunto não vazio. Uma operação binária $*$ é uma função de $G \times G$ em G, tal que:

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto a * b. \end{aligned}$$

Isso significa dizer que todo par $(a, b) \in G \times G$ possui um único elemento do contradomínio de G.

Exemplo 2.2. A função $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por $f(a, b) = a + b$ é uma operação de adição em $\mathbb{Z}$, pois $f(2, 7) = 2 + 7 = 9$. Ademais, temos $g(a, b) = a \cdot b$ como uma operação de multiplicação, pois $f(2, 7) = 2 \cdot 7 = 14$. Estas operações podem sem estendidas para os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

Exemplo 2.3. A função $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, com $f(a, b) = \frac{a}{b}$ não está bem definida, pois $f(2, 3) \in \mathbb{Z} \times \mathbb{Z}$, porém $f(2, 3) = \frac{2}{3} \notin \mathbb{Z}$.

2.2 Grupos

Desde cedo, nos familiarizamos com conjuntos numéricos, como os conjuntos dos números naturais $\mathbb{N}$, inteiros $\mathbb{Z}$, racionais $\mathbb{Q}$ e reais $\mathbb{R}$. Dentro desses conjuntos, ao considerar a operação de adição, algumas propriedades se destacam: a associatividade, que nos permite realizar somas sem nos preocupar com a ordem dos parênteses; a existência de um elemento neutro, pois adicionar 0 a qualquer número não altera o valor do número; e a existência de inversos, onde somar um número x com o seu oposto $-x$ resulta em 0. Naturalmente, surgem algumas questões:

- Essas propriedades se mantêm em outros conjuntos numéricos?
- Tais características se aplicam a outros conjuntos, como os conjuntos de matrizes, polinômios ou funções?
- E se considerarmos outras operações, como multiplicação, potenciação ou composição?

Essas perguntas buscam entender melhor a natureza de uma operação específica em um determinado conjunto. Em outras palavras, desejamos investigar as propriedades algébricas que surgem ao associar operações a conjuntos, e a partir dessas observações, podemos identificar estruturas comuns que se repetem em diversos contextos matemáticos. Como veremos na definição a seguir, um conjunto dotado de uma operação que satisfaz as propriedades listadas acima recebe uma designação especial na álgebra abstrata: ele é chamado de grupo.

Definição 2.4. Seja G um conjunto não vazio munido de uma operação $*$. Dizemos que $(G, *)$ é um grupo quando as seguintes propriedades são satisfeitas:

1. Associatividade: $(a * b) * c = a * (b * c)$, para todo $a, b, c \in G$;
2. Existência do elemento neutro: existe $e \in G$, tal que $e * a = a * e = a$, para todo $a \in G$;
3. Existência do elemento simétrico (ou inverso): para todo $a \in G$, existe $a' \in G$, tal que $a' * a = a * a' = e$.

Observação 2.5.

- É comum a operação $*$ ser denotada simplesmente por $\cdot$ e a operação entre dois elementos a e b por $a \cdot b$ ou, simplesmente, ab. Neste caso, o grupo G é dito multiplicativo (ou que está na notação multiplicativa);
- Quando a operação do grupo for denotada por $+$, a operação entre dois elementos a e b será denotada por $a + b$ (neste caso, o grupo é chamado de aditivo ou que está na notação aditiva);

- Quando não houver dúvidas sobre a operação do grupo, o grupo será denotado simplesmente por G.

Exemplo 2.6. Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ munidos da adição usual são exemplos de grupos.

Exemplo 2.7. Considerando a multiplicação usual, os conjuntos do exemplo 2.6 não são grupos, pois o elemento 0 não tem inverso multiplicativo. Ora, como dado $x \neq 0$ ele possui inverso nos conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ (tal inverso é dado por $1/x$), e a operação de multiplicação cumpre as demais propriedades que exigimos na definição de grupo, temos $(\mathbb{R}^*, \cdot), (\mathbb{Q}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$ grupos, em que $\cdot$ é a multiplicação usual.

Exemplo 2.8. O conjunto dos números inteiros com a operação de subtração não é um grupo. De fato, tomando $1, 2, 7 \in \mathbb{Z}$, temos $1 - (2 - 7) = 1 + 5 = 6$. Por outro lado, $(1 - 2) - 7 = -1 - 7 = -8$. Ou seja, a propriedade de associatividade da operação, como exigida na Definição 2.4, não foi satisfeita. Portanto, $(\mathbb{Z}, -)$ não é um grupo.

Exemplo 2.9. O conjunto de todas as matrizes de ordem n com entrada no conjunto dos números reais, denotado por $M_n(\mathbb{R})$, munido da adição usual é um grupo.

Exemplo 2.10. O conjunto de todas as matrizes de ordem 2, denotado por $M_2(\mathbb{R})$, munido da multiplicação usual não é um grupo, pois, embora saibamos que na multiplicação usual de matrizes a associatividade e a existência do elemento neutro sejam válidos, em alguns casos a existência do elemento inverso não é satisfeita.

Ora, sabemos que uma matriz é inversível se, e somente se, seu determinante é não nulo. Assim, o conjunto $GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid det(A) \neq 0\}$ satisfaz todas as condições exigidas na Definição 2.4, basta apenas mostrarmos que $GL_2(\mathbb{R})$ é fechado sob a multiplicação. Consideremos então $X, Y \in GL_2(\mathbb{R})$, ou seja, $detX \neq 0$ e $detY \neq 0$. Pelo Teorema de Binet, obtemos que o produto dos determinantes das matrizes é o determinante do produto, logo $detX \cdot detY = det(X \cdot Y) \neq 0$, isto é, $X \cdot Y \in GL_2(\mathbb{R})$. Portanto, $GL_2(\mathbb{R})$ é fechado sob a multiplicação. Deste modo, $(GL_2(\mathbb{R}), \cdot)$ é um grupo. Esse grupo é chamado de grupo geral linear de grau 2 sobre $\mathbb{R}$ e, note que, tal resultado pode ser generalizado para matrizes de ordem $n \in \mathbb{N}$ qualquer.

Observando os exemplos acima, percebe-se que nem todas as operações tratadas satisfazem a comutatividade, isto é, a ordem dos elementos, ás vezes, não altera o resultado da operação. Este é o caso do produto de matrizes: nem sempre dadas duas matrizes A e B, quadradas e de mesma ordem, satisfaz $AB = BA$. De modo mais geral, os grupos cuja operação satisfaz a comutatividade recebem um nome especial e é formalizado na definição a seguir.

Definição 2.11. Um grupo $(G, \cdot)$ é chamado de comutativo (ou abeliano) quando a operação em G for comutativa. Ou seja, para quaisquer $a, b \in G$, vale $a \cdot b = b \cdot a$.

Exemplo 2.12. Exemplos clássicos de grupos abelianos: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ e $(\mathbb{C}, +)$. Como também temos $(\mathbb{R}^*, \cdot), (\mathbb{Q}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$.

2.3 Grupo de Classes Residuais

Dados $a, b, n \in \mathbb{Z}$, com $n > 1$. A relação de congruência $a \equiv b(mod\ n)$ se, e somente se, $a - b = kn$, para algum, $k \in \mathbb{N}$, define uma relação de equivalência em $\mathbb{Z}$. Podemos mostrar que dois inteiros quaisquer são equivalentes quando o resto da divisão euclidiana deles por n são as mesmas. Diante disso, dizemos que uma classe de resto, ou residual, é o conjunto de todos os inteiros que resultam o mesmo resto quando são divididos pelo inteiro positivo n.

O conjunto dessas classes é finito e será denotado por $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. Tal conjunto é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo n, de modo que, pelo algoritmo euclidiano, o resto r é obrigatoriamente $0 \leq r < n$.

A proposição a seguir é um resultado já conhecido em disciplinas como Teoria dos Números, mas com o intuito de deixar o nosso trabalho o mais auto-contido possível, faremos a sua demonstração.

Proposição 2.13. As operações de adição e multiplicação, sobre $\mathbb{Z}_n$, têm as seguintes propriedades:

1. $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$, para todo $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$;

2. Dado $\overline{a} \in \mathbb{Z}_n$, existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, se, e somente se, o $mdc(a, n) = 1$. ($\overline{a}$ tem inverso multiplicativo).

Demonstração. 1. Considerando $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, com a associatividade válida na multiplicação em $\mathbb{Z}$, temos:

$$\begin{aligned} \overline{a} \cdot (\overline{b} \cdot \overline{c}) &= \overline{a} \cdot (\overline{b \cdot c}) \\ &= \overline{a \cdot (b \cdot c)} \\ &= \overline{(a \cdot b) \cdot c} \\ &= \overline{(a \cdot b)} \cdot \overline{c} \\ &= (\overline{a} \cdot \overline{b}) \cdot \overline{c} \end{aligned}$$

2. Dado $\overline{a} \in \mathbb{Z}_n$, suponha que exista $\overline{b} \in \mathbb{Z}_n$, de modo que $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{1}$. Logo, $a \cdot b \equiv 1(mod\ n)$, ou seja,

$$a \cdot b + k \cdot n = 1, com\ k \in \mathbb{Z}$$

Portanto, temos $mdc(a, n) = 1$.

Reciprocamente, pela identidade de Bézout[1], temos

$$\begin{aligned}\overline{a\cdot x+n\cdot y}=\overline{1}&\Leftrightarrow \overline{a\cdot x}+\overline{n\cdot y}=\overline{1}\\&\Leftrightarrow \overline{a}\cdot\overline{x}+\overline{n}\cdot\overline{y}=\overline{1}\\&\Leftrightarrow \overline{a}\cdot\overline{x}+\overline{0}\cdot\overline{y}=\overline{1}\end{aligned}$$

Isto é, $\overline{a}\cdot\overline{x}=\overline{1}$. Portanto, $\overline{a}$ possui inverso multiplicativo. □

Munido desta proposição, estudemos melhor o conjunto $\mathbb{Z}_n$.

Exemplo 2.14. O conjunto $\mathbb{Z}_n$, quando $n\geq 2$ na multiplicação usual, não é grupo. Pois a cada valor atribuído a n, podendo ser $n=\{2,3,4,\ldots\}$ sabemos que $\mathbb{Z}_n$ terá $\overline{0}$ em todos os casos como elemento. Porém, $\overline{0}$ não possui elemento inverso na multiplicação, pois supondo que existe $\overline{a}\in\mathbb{Z}_n$ tal que $\overline{0}\cdot\overline{a}=\overline{1}$. Mas, tal igualdade em $\mathbb{Z}_n$ implica que $mdc(0,1)=1$, o que é um absurdo. Logo, não é grupo. Por outro lado, se tomarmos o subconjunto próprio $U(\mathbb{Z}_n)$ de $\mathbb{Z}_n$, dado por

$$U(\mathbb{Z}_n)=\{\overline{a}\in\mathbb{Z}_n; mdc(a,n)=1\},$$

pelos itens da Proposição 2.13 teremos que o subconjunto próprio $U(\mathbb{Z}_n)$ é um grupo.

De fato, pelo que foi exposto na Proposição 2.13, basta mostrarmos apenas a existência do elemento neutro. $\overline{x}\in U(\mathbb{Z}_n)$. Ora, mas veja que

$$\overline{x}\cdot\overline{1}=\overline{x\cdot 1}=\overline{x}$$
$$\overline{1}\cdot\overline{x}=\overline{1\cdot x}=\overline{x}$$

Logo, $\overline{1}$ é o elemento neutro de $U(\mathbb{Z}_n)$ com a multiplicação usual.

Exemplo 2.15. Seja A um conjunto não vazio. Dizemos que $S_A=\{f:A\to A; f$ é uma bijeção$\}$ é o conjunto de todas as permutações de A. Ao munir S_A com a operação $\circ$, onde $(f\circ g)(x)=f(g(x))$, para todo $x\in S_A$, verificaremos que as propriedades exigidas na definição de grupo são satisfeitas:

1. Associatividade: Dados, $f,g,h\in S_A$, temos

$$[(f\circ g)\circ h](x)=[f\circ(g\circ h)](x),\forall x\in A.$$

[1]Bachet-Bézout foi um matemático francês, contribuiu bastante para a Teoria dos Números com um teorema muito importante que leva seu nome.

Isso implica

$$\begin{aligned}[(f \circ g) \circ h](x) &= f(g(x)) \circ h(x) \\ &= f(g(h(x))) \\ &= f[(g \circ h)(x)] \\ &= [f \circ (g \circ h)](x), \forall x \in A.\end{aligned}$$

Portanto, é válida a associatividade.

2. Elemento neutro: Dado $f \in S_A$, vamos mostrar que existe $g \in S_A$ de modo que

$$(f \circ g)(x) = e = (g \circ f)(x).$$

Considere $id \in S_A$, onde $id(x) = x$, para todo $x \in S_A$. Note que id satisfaz a condição acima, pois

$$\begin{aligned}f \circ id(x) &= f(id(x)) \\ &= f(x).\end{aligned}$$

Da mesma forma, segue para

$$\begin{aligned}id \circ f(x) &= id(f(x)) \\ &= f(x).\end{aligned}$$

Logo, a função identidade é o elemento neutro da operação.

3. Elemento simétrico: Dado $f \in S_A$, iremos provar que existe $f' \in S_A$ tal que

$$[f \circ f'](x) = id = [f' \circ f](x).$$

Note que, como f é bijetora, existe $f^{-1} \in S_A$, tal que

$$f \circ f^{-1} = f^{-1} \circ f = id.$$

Logo, a função f^{-1} procurada é a inversa de f. Portanto, $(S_A, \circ)$ é um grupo.

Se $A = \{1, 2, \ldots, n\}$, então S_A será denotado por S_n e chamado de grupo simétrico de grau n. Por exemplo, S_3 é um grupo com seis elementos, com a operação de composição de funções. Neste exemplo, denotaremos a operação de composição $\alpha \circ \beta$, por simplesmente $\alpha\beta$. Assim, considerando o conjunto $A = \{1, 2, 3\}$, vamos efetuar alguns produtos $\alpha\beta$, com

$\alpha, \beta \in S_3$. Daí, teremos as seguintes permutações de A:

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

com $S_3 = \{\alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4,\ \alpha_5,\ \alpha_6\}$. A partir disso, tomando $\alpha = \alpha_6$ e $\beta = \alpha_2$, de modo que

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha_5,$$

$$\alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = e,$$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = e,$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha_3,$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha_4.$$

Observe que os elementos do grupo S_3 podem ser gerados a partir de combinações dos fatores α e β, levando em conta que $\alpha = e \cdot \alpha$ e $\beta = e \cdot \beta$, onde e representa o elemento neutro do grupo. Isso significa que, através da aplicação de operações envolvendo α e β, conseguimos gerar todos os elementos do grupo S_3. Em outras palavras, α e β são geradores do grupo S_3, ou seja, qualquer elemento de S_3 pode ser expresso como um produto de potências de α e β.

Definição 2.16. Definimos a ordem do grupo G como a quantidade de elementos do conjunto G, e denotamos a ordem de um grupo G por $|G|$. Caso G tenha infinitos elementos, dizemos que G tem ordem infinita.

Exemplo 2.17. O conjunto $G = \{-1, 1\}$ com a operação de multiplicação usual é um grupo abeliano, com $|G| = 2$.

Exemplo 2.18. Os grupos $\mathbb{Z}$ e $\mathbb{R}$ com a adição usual têm ordem infinita.

Exemplo 2.19. O conjunto $2\mathbb{Z}$ de todos os inteiros pares, com a adição usual, é um grupo de ordem infinita.

Exemplo 2.20. O grupo $\mathbb{Z}_n$, sob a adição usual, possui ordem finita, com $|\mathbb{Z}_n| = n$.

A resolução do exemplo acima se encontra na referência (7) deste trabalho.

2.4 Propriedades Elementares de um Grupo

Nesta seção, exploramos de forma mais geral propriedades conhecidas, como a lei do cancelamento e as propriedades da potenciação. Essas características, embora familiares no contexto de números, assumem um papel central e mais profundo ao serem consideradas em estruturas algébricas como os grupos. A teoria de grupos oferece uma estrutura que generaliza e amplia o entendimento dessas propriedades, permitindo-nos enxergá-las sob uma ótica mais abstrata e aplicável a diferentes contextos. Assim, o estudo de grupos possibilita uma visão unificada e abrangente de temas já introduzidos no ensino básico, mas agora expandidos e aplicáveis a estruturas matemáticas mais amplas, enriquecendo a compreensão de operações.

Proposição 2.21. Seja $(G, \cdot)$ um grupo. As leis do cancelamento à esquerda e à direita são válidas em G. Isto é, dados $a, b, c \in G$,

$$a \cdot b = a \cdot c \Rightarrow b = c \text{ e } b \cdot a = c \cdot a \Rightarrow b = c.$$

Demonstração. Dado $a \in G$, existe $a' \in G$, tal que $a' \cdot a = e = a \cdot a'$. Então,

$$a \cdot b = a \cdot c \Rightarrow a' \cdot (a \cdot b) = a' \cdot (a \cdot c).$$

Da associatividade da operação, segue que:

$$(a' \cdot a) \cdot b = (a' \cdot a) \cdot c,$$

daí,

$$e \cdot b = e \cdot c,$$

ou seja, $b = c$.

Analogamente, temos

$$\begin{aligned} b \cdot a = c \cdot a &\Rightarrow (b \cdot a) \cdot a' = (c \cdot a) \cdot a', \\ &\Rightarrow b \cdot (a \cdot a') = c \cdot (a \cdot a'), \end{aligned}$$

isto é, $b = c$. Portanto, as leis do cancelamento são válidas.

□

Proposição 2.22. Seja $(G, \cdot)$ um grupo. Então,

1. existe um único elemento $e \in G$, tal que

$$e \cdot a = a \cdot e = a, \text{ para todo } a \in G.$$

2. para cada $a \in G$, existe um único $a' \in G$, tal que

$$a' \cdot a = a \cdot a' = e.$$

Demonstração. 1. Considere $e_1, e_2 \in G$, tais que

$$a \cdot e_1 = a = e_1 \cdot a, \forall a \in G, \tag{2.1}$$
$$a \cdot e_2 = a = e_2 \cdot a, \forall a \in G, \tag{2.2}$$

em particular,

$$e_1 \cdot e_2 = e_1, e_1 \cdot e_2 = e_2.$$

ou seja,

$$e_1 = e_1 \cdot e_2 = e_2.$$

Portanto, o elemento neutro em G é único.

2. Seja $a \in G$, suponha que existem $a', a'' \in G$, tais que a', a'' são os inversos de a. Daí,

$$\begin{aligned} a \cdot a' = e &\Rightarrow a'' \cdot (a \cdot a') = a'' \cdot e \\ &\Rightarrow e \cdot a' = a'' \\ &\Rightarrow a' = a''. \end{aligned}$$

Da mesma forma segue para a'' à direita. Portanto, para cada $a \in G$ existe um único inverso.

□

Proposição 2.23. Em um grupo $(G, \cdot)$, valem:

1. $(a')' = a$, para todo $a \in G$;
2. $(a \cdot b)' = b' \cdot a'$, para todo $a, b \in G$.

Demonstração. 1. Basta notar que

$$\begin{aligned} a' \cdot (a')' = e &\Rightarrow a \cdot a' \cdot (a')' = a \cdot e \\ &\Rightarrow (a')' = a. \end{aligned}$$

2. Para provar o desejado, basta mostrarmos que

$$(a \cdot b) \cdot (b' \cdot a') = e.$$

Como G é grupo, é válida a associatividade. Logo,

$$\begin{aligned}(a\cdot b)\cdot(b'\cdot a') &= a\cdot(b\cdot b')\cdot a'\\ &= a\cdot e\cdot a'\\ &= a\cdot a'\\ &= e.\end{aligned}$$

Portanto, $(a\cdot b)' = b'\cdot a'$.

□

Observação 2.24. Em alguns casos a seguir, denotaremos os invertíveis de um grupo por a^{-1}, o motivo desta alteração é para seguirmos as notações já conhecidas ao tratarmos com potências de um número.

Definição 2.25. (Potências e Múltiplos de um Grupo) Seja $(G,\cdot)$ um grupo. Dados $a\in G$ e $n\in\mathbb{Z}$, a n-ésima potência de a é dada da seguinte forma:

$$a^n = \begin{cases} e, \text{ se } n = 0\\ a^{n-1}\cdot a, \text{ se } n > 0\\ (a^{-n})^{-1}, \text{ se } n < 0\end{cases}$$

Se a operação em G for aditiva, então definimos os múltiplos de a, em símbolos $n\cdot a$ como

$$n\cdot a = \begin{cases} e, \text{ se } n = 0\\ (n-1)\cdot a + a, \text{ se } n > 0\\ (-n)\cdot(-a), \text{ se } n < 0\end{cases}$$

A demonstração da proposição a seguir se encontra na referência (7) deste trabalho.

Proposição 2.26. Seja $(G,\cdot)$ um grupo. Dados $a\in G$ e $n,m\in\mathbb{Z}$, temos:

1. $a^n\cdot a^m = a^{n+m}$.
2. $(a^n)^m = a^{nm}$.

2.5 Subgrupos

Ao estudar grupos, uma questão que surge naturalmente é se é possível encontrar subconjuntos que, por si mesmos, mantenham a estrutura de grupo. Em outras palavras, dado um grupo, será que existe um subconjunto que também seja um grupo sob a mesma operação? Esse tipo de estrutura interna, chamada de subgrupo, é essencial para entender a organização dos elementos e a dinâmica das operações dentro de um grupo maior. Os

subgrupos revelam simetrias e padrões que podem simplificar problemas complexos e fornecer uma visão mais detalhada da estrutura do grupo original.

A definição de subgrupo nos permite, então, identificar subconjuntos que preservam as propriedades essenciais de um grupo: fechamento, existência de elemento neutro, associatividade e inversos. Esses subgrupos desempenham um papel fundamental na teoria de grupos, pois, além de facilitarem o estudo de grupos maiores, também abrem caminho para conceitos avançados, como as classes laterais e os quocientes, que aprofundam nossa compreensão das relações entre diferentes grupos.

Definição 2.27. Sejam $(G, \cdot)$ um grupo e H um subconjunto de G. Dizemos que H é um subgrupo de G, e denotamos por $H < G$, quando H, munido da operação de G, também é um grupo.

Observação 2.28.

Exemplo 2.29. Em um grupo G qualquer, temos como subgrupos $H_1 = \{e\}$ e $H_2 = G$, denominados subgrupos triviais de G. Quando H não é um subgrupo trivial, dizemos que H é subgrupo próprio.

Exemplo 2.30. São exemplos clássicos de subgrupos sob a adição usual $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. Já na multiplicação usual, temos $\mathbb{Z}^* < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$

Exemplo 2.31. $(\mathbb{Q}^*, \cdot)$ não é subgrupo de $(\mathbb{R}^*, +)$, mesmo que $\mathbb{Q}^* \subset \mathbb{R}$. O motivo para isso ocorrer é o fato de que a operação em $\mathbb{Q}^*$ e $\mathbb{R}$ são distintas. O mesmo ocorre para os casos de $(\mathbb{Z}, +)$ não ser subgrupo de $(\mathbb{Q}^*, \cdot)$, ou até $(\mathbb{Z}^*, \cdot)$ não ser subgrupo de $(\mathbb{Q}, +)$.

Proposição 2.32. Sejam G um grupo e H um subgrupo de G. Então,

1. A identidade de H, denotada por e_H, é igual a identidade de G.
2. Dado $h \in H$, o inverso de h em H coincide com o inverso de h em G.

Demonstração. 1. Dado $h \in H$, existe $h^{-1} \in G$, tal que $h \cdot h^{-1} = e = h^{-1} \cdot h$. Mas,

$$\begin{aligned} h \cdot e_H = h &\Rightarrow h^{-1} \cdot e_H = h^{-1} \cdot h \\ &\Rightarrow e_H = e. \end{aligned}$$

Note que, da mesma forma que foi verificada a identidade à esquerda, segue os mesmos procedimentos à direita, resultando na igualdade. Portanto a identidade de H e G são iguais.

2. Considerando h^{-1} o inverso de h em H, temos

$$h \cdot h^{-1} = e_H$$

Pelo item 1., a identidade de H coincide com a de G. Daí, h^{-1} é o inverso de h em G e, portanto, o inverso de h em H e G são iguais.

□

Teorema 2.33. Seja H um subconjunto não vazio de um grupo G, H é subgrupo de G se, e somente se, uma das seguintes condições é satisfeita:

1. $h_1 \cdot h_2 \in H$ e $h_1^{-1} \in H,\ \forall\ h_1, h_2 \in H$.
2. $h_1 \cdot h_2^{-1} \in H,\ \forall\ h_1, h_2 \in H$.

Demonstração. Como H é um subgrupo de G, segue que H também é um grupo. E por esta razão as condições acimas são satisfeitas.

1. Suponha que H satisfaz a condição 1. Assim, para todo $h \in H$ existe $h^{-1} \in H$. Isso implica que $h \cdot h^{-1} = e \in H$. Logo, $H < G$.
2. Agora, suponha que H satisfaz a condição 2. Logo, tomando $h_1, h_2 \in H$, temos

$$h_2 \cdot h_2^{-1} = e \in H.$$

Assim, aplicando a condição 2. novamente, segue que $e \cdot h_2^{-1} \in H$ e, deste modo, H é fechado para inversos. Por fim, note que

$$h_2^{-1} = e \cdot h_2^{-1} \in H.$$

Deste modo, segue que

$$h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \text{ em } H.$$

Portanto, H é subgrupo de G.

□

Vejamos uma aplicação da proposição acima.

Exemplo 2.34. O conjunto $2\mathbb{Z}$ de todos os inteiros pares (múltiplos de 2),

$$2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$$

é um subgrupo de $(\mathbb{Z}, +)$.

De fato, considere $x, y \in 2\mathbb{Z}$, tais que $x = 2k_1$, $y = 2k_2$, com $k_1, k_2 \in \mathbb{N}$. Assim, o inverso de y será $-y = -2k_2$. Para $x + y$, teremos que

$$\begin{aligned} x + y &= 2k_1 + 2k_2 \\ &= 2(k_1 + k_2) \in \mathbb{Z}. \end{aligned}$$

Para $x + (-y)$, teremos que

$$\begin{aligned} x + (-y) &= 2k_1 - 2k_2 \\ &= 2(k_1 - k_2) \in \mathbb{Z}. \end{aligned}$$

Portanto, $2\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$.

Exemplo 2.35. Percebe-se que, no exemplo anterior, é possível considerar subconjuntos H de $\mathbb{Z}$ formados por um múltiplo qualquer além do 2, e ainda obter $H < \mathbb{Z}$. Ou seja, para cada $n \in \mathbb{Z}$, o conjunto $H = n\mathbb{Z}$ (múltiplos de n) denotado por

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

é subgrupo de $\mathbb{Z}$.

Proposição 2.36. (Os Subgrupos de $\mathbb{Z}$) Seja H um subconjunto não vazio de $\mathbb{Z}$. Então, H é um subgrupo de $\mathbb{Z}$ se, e somente se, existe $n \in \mathbb{Z}$ tal que $H = n\mathbb{Z}$.

Demonstração. A partir do Exemplo 2.35, para cada $n \in \mathbb{Z}$, o conjunto $H = n\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$. Analogamente, seja H um subgrupo de $\mathbb{Z}$. Se $H = 0$, então $H = \{0\}\mathbb{Z}$. Por este motivo, vamos supor que $H \neq 0$.

Considere $a \in H$, com $a \neq 0$. Como $H < \mathbb{Z}$, então $-a \in H$. Assim, $W = \{a \in H : a > 0\}$ é não vazio. Consideremos, de acordo com o PBO,

$$n = minW.$$

Vamos mostrar que $H = n\mathbb{Z}$. Como $n \in H$, então $nk \in H$ para todo $k \in \mathbb{Z}$, pois

$$k \cdot n = \begin{cases} n + \cdots + n, & (k \text{ vezes , com } k > 0) \\ -n - \cdots - n, & (|k| \text{ vezes , com } k < 0) \end{cases}$$

Desse modo, $n\mathbb{Z} \subset H$. Ademais, pelo algoritmo da divisão, dado $h \in H$, existem $q, r \in \mathbb{Z}$ tais que

$$h = nq + r, \text{ com } \ 0 \leqslant \ r < n.$$

Logo, $r = h - nq \in H$, pois $h, nq \in H$. Mas, como $\ 0 \leqslant \ r < n$, então pela minimalidade de n, devemos ter $r = 0$. Portanto, $h = nq \in n\mathbb{Z}$, ou seja, $H \subset n\mathbb{Z}$ e $H = n\mathbb{Z}$.

□

Teorema 2.37. Sejam G um grupo e H um subconjunto finito não vazio de G . Então,

$$H < G \Leftrightarrow h_1 \cdot h_2 \in H, \forall \ h_1, h_2 \in H.$$

Demonstração. $\Rightarrow$) Segue de imediato pelo Teorema 2.33 que H é um subgrupo, pois $h_1 \cdot h_2 \in H, \forall\ h_1, h_2 \in H$.

Suponha que H seja fechado sob a operação em G. Pelo Teorema 2.33 , basta mostrar que H é fechado para os inversos. Com isso, dado $h \in H$, vamos provar que $h^{-1} \in H$. Suponha que $|H| = n$, note que, $h, h^2, h^3, \ldots, h^{n+1} \in H$. É válido ressaltar que os $n+1$ elementos não são todos distintos, uma vez que H possui n elementos. Logo, existem $i, j \in \{1, 2, \ldots, n+1\}$, com $i < j$, tais que

$$h^j = h^i.$$

Multiplicando ambos os membro desta igualdade por h^{-i}, obtemos

$$e = h^{j-i} \in H.$$

Por isso,

$$h^{-1} \cdot e = h^{j-i} \Rightarrow h^{-1} = h^{j-i-1} \in H.$$

Portanto, H é subgrupo de G.

□

Exemplo 2.38. Sejam G um grupo qualquer e $Z(G)$ o subconjunto de G cujos elementos comutam com todo elemento de G, ou seja

$$Z(G) = \{a \in G : xa = ax, \forall x \in G\}.$$

Vamos mostrar que $Z(G)$ é um subgrupo de G. Para isso, considere $a, b \in Z(G)$ e $x \in G$, daí,

$$\begin{aligned}(a \cdot b^{-1}) \cdot x &= (a \cdot b^{-1}) \cdot x \cdot e \\ &= a \cdot b^{-1} \cdot x \cdot b \cdot b^{-1} \\ &= a \cdot b^{-1}\ b \cdot x \cdot b^{-1}, \text{pois } b \in Z(G) \\ &= a \cdot x \cdot b^{-1} \\ &= x\ (a \cdot b^{-1}), \text{pois } a \in Z(G).\end{aligned}$$

Ou seja,

$$(a \cdot b^{-1})\ x = x\ (a \cdot b^{-1}).$$

Portanto, $a \cdot b^{-1} \in Z(G)$ e, assim, $Z(G) < G$.

Proposição 2.39. Se H_1 e H_2 são subgrupos de um grupo G, então $H_1 \cap H_2$ é um subgrupo de G.

Demonstração. Se H_1 e H_2 são subgrupos de G, significa que não são vazios e que $e \in H_1 \cap H_2$. Com isso, considere $x, y \in H_1 \cap H_2$, temos

$$x \in H_1 \text{ e } y \in H_1 \Rightarrow y^{-1} \text{ e } xy^{-1} \in H_1, \text{ pois } H_1 < G,$$
$$x \in H_2 \text{ e } y \in H_2 \Rightarrow y^{-1} \text{ e } xy^{-1} \in H_2, \text{ pois } H_2 < G.$$

Portanto, $xy \in H_1 \cap H_2$. □

2.6 Grupos Diedrais

Os grupos que serão apresentados abaixo são utilizados para descrever simetrias em formas geométricas, seja triângulos, quadrados ou polígonos regulares. Eles são considerados grupos não abelianos por não satisfazer a comutatividade na operação binária. Estes grupos são classes importantes dos Grupos de Permutação, conhecidos como Grupos Diedrais.

Definição 2.40. O grupo Diedral, denotado por D_n, é um grupo de simetrias espaciais de um polígono regular de n lados iguais.

Seja $A_1A_2A_3 \ldots A_n$ um polígono regular de n lados e sejam $E_1, E_2, \ldots, E_n$ seus eixos. Considerando o conjunto de transformações espaciais que preservam o polígono com a operação de composição, temos:

- $e, R_{\frac{2\pi}{n}}, \ldots, R_{\frac{2(n-1)\pi}{n}}$ as rotações do plano em torno do centro do polígono, no sentido anti-horário de ângulos $0, \frac{2\pi}{n}, \ldots, \frac{2(n-1)\pi}{n}$.
- $R_1, R_2, \ldots, R_n$ as rotações espaciais de ângulo com os eixos $E_1, E_2, \ldots, E_n$.

Observação 2.41. D_n é um grupo não abeliano, munido da operação de composição, pois não há comutatividade entre as rotações planas e especiais ao serem combinadas.

A demonstração do teorema a seguir se encontra na referência (7) deste trabalho.

Teorema 2.42. O grupo Diedral D_n é um grupo de ordem 2n gerado por dois elementos α e β, satisfazendo $\alpha^n = \beta^2 = e$, em que:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$

Observa-se também que o grupo D_n, contém ele próprio um subgrupo de ordem n. Com efeito,

$$R_n = \{e, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

é um subgrupo de D_n, com ordem n.

Exemplo 2.43. O grupo D_3 com a operação de composição de funções é um grupo não abeliano. Seja $A_1A_2A_3$ um triângulo equilátero com E_1, E_2, E_3 seus eixos, temos

- $e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}$ as rotações do plano em torno do centro do triângulo equilátero, no sentido anti-horário de ângulos $0, \frac{2\pi}{3}, \frac{4\pi}{3}$.
- R_1, R_2, R_3 as rotações espaciais de ângulo com os eixos E_1, E_2, E_3.

Logo, $D_3 = \{e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$ com a operação de composição é um grupo.

Exemplo 2.44. O grupo D_4 com a operação de composição de funções é um grupo não abeliano. Seja $A_1A_2A_3, A_4$ um quadrado com E_1, E_2, E_3, E_4 seus eixos, temos

- $e, R_{\frac{\pi}{2}}, R_{\pi}, \frac{3\pi}{2}$ as rotações do plano em torno do centro do quadrado, no sentido anti-horário de ângulos $0, \frac{\pi}{2}, \pi\frac{3\pi}{2}$.
- R_1, R_2, R_3 as rotações espaciais de ângulo com os eixos E_1, E_2, E_3.

Portanto, $D_4 = \{e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$ com a operação de composição é um grupo.

2.7 Grupos cíclicos

Para entender a ideia de um grupo cíclico, podemos considerar um exemplo familiar: o conjunto formado pelas potências da unidade imaginária i nos números complexos. Sabemos que i representa a raiz quadrada de -1, e as potências de i seguem um padrão cíclico interessante:

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1, \quad i^5 = -i, \quad i^6 = -1, \text{etc.}$$

Notamos que, ao atingir $i^4 = 1$, o ciclo recomeça, e qualquer potência de i pode ser reduzida a um desses quatro valores: i, -1, $-i$ e 1. Esse conjunto de elementos, $\{1, i, -1, -i\}$, junto com a operação de multiplicação, forma um grupo. Curiosamente, todos os elementos deste grupo podem ser obtidos apenas a partir de i e suas potências sucessivas.

Esse exemplo nos leva ao conceito de grupo cíclico: um grupo em que todos os elementos podem ser gerados a partir de um único elemento, chamado de gerador. No caso do conjunto das potências de i, i é o gerador do grupo, pois basta combiná-lo consigo mesmo para recuperar todos os outros elementos. Grupos cíclicos como esse oferecem uma estrutura mais simples e elegante para o estudo da teoria de grupos, permitindo que exploremos propriedades profundas usando apenas um elemento fundamental para gerar todo o grupo. Vejamos a seguir a definição formal desse conceito.

Definição 2.45. Seja G um grupo e $a \in G$. Denotamos por $< a >$ o subconjunto de G, formado por todas as potências inteiras de a, isto é

$$< a > = \{a^m; m \in \mathbb{Z}\}.$$

Dizemos que G é um grupo cíclico se, existe $a \in G$, tal que $G = < a >$, ou seja

$$G = \{a^m; m \in \mathbb{Z}\}.$$

Neste caso, dizemos que a é um gerador do grupo G.

Observação 2.46. Para um grupo cíclico $G = < a >$ há duas possibilidades:

1. $a^n = e$ para algum $n \in \mathbb{N}$. Neste caso, G tem ordem finita.
2. $a^n \neq e$ para todo $n \in \mathbb{N}$. Neste caso, todas as potências de a são distintas e G tem ordem infinita.

Além disso, para um grupo G cíclico munido da operação da adição usual, ou seja $(G, +)$ com $a \in G$, temos que:

$$G = \{n \cdot a; n \in \mathbb{Z}\}$$

Exemplo 2.47. Como já vimos no início da seção, o grupo $G = \{1, -1, i, -i\}$ munido da multiplicação usual de números complexos é cíclico gerado por i. Note que $-i$ também é um gerador para este grupo.

Exemplo 2.48. O grupo $G = (\mathbb{Z}, +)$ é cíclico. Basta notar que com $a = 1$ temos,

$$< 1 > = \{n \cdot 1;\ n \in \mathbb{Z}\}\ = \{n;\ n \in \mathbb{Z}\} = \mathbb{Z}.$$

Portanto, $\mathbb{Z} = < 1 >$. Além disso, também vale $\mathbb{Z} = < -1 >$.

Exemplo 2.49. Para cada $n \in \mathbb{Z}$, o grupo $(\mathbb{Z}_n, +)$ é cíclico.

Exemplo 2.50. O grupo $G = (\mathbb{Q}, +)$ não é cíclico. De fato, suponhamos que G seja cíclico. Desse modo, existe $\frac{a}{b} \in \mathbb{Q}$ tal que $G = < \frac{a}{b} >$. Como $\frac{a}{2b} \in \mathbb{Q}$, existe $n \in \mathbb{Z}$ tal que

$$\frac{a}{2b} = n \cdot \frac{a}{b}.$$

Ora, mas isso implica que $n = \dfrac{1}{2}$, o que é um absurdo, pois $n \notin \mathbb{Q}$. Logo, $(\mathbb{Q}, +)$ não é um grupo cíclico.

Exemplo 2.51. O grupo $U(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\}$ é cíclico, pois $U(\mathbb{Z}_4) = < 3 >$.

Note que, ao tomarmos $\overline{1}$, estariamos apenas gerando ele próprio do grupo. Agora, ao tomar $\overline{3}$, temos

$$\overline{3^2} = \overline{9} = \overline{1} \in U(\mathbb{Z}_4).$$
$$\overline{3^3} = \overline{27} = \overline{3} \in U(\mathbb{Z}_4).$$

Portanto, $< 3 >$ é o gerador de $U(\mathbb{Z}_4)$.

Proposição 2.52. Todo grupo cíclico é abeliano.

Demonstração. Sejam G um grupo cíclico e $a \in G$, tal que

$$G = < a > = \{a^n;\ n \in \mathbb{Z}\}.$$

Tome $x_1, x_2 \in G$, tais que $x_1 = a^{n_1}$ e $x_2 = a^{n_2}$. Então, temos que

$$\begin{aligned} x_1 \cdot x_2 &= a^{n_1} \cdot a^{n_2} \\ &= a^{n_1+n_2} \\ &= a^{n_2+n_1} \\ &= a^{n_2} \cdot a^{n_1} \\ &= x_2 \cdot x_1 \end{aligned}$$

Portanto, G é abeliano.

□

Definição 2.53. Sejam G um grupo e $a \in G$. Dizemos que o elemento a tem ordem finita, quando existe $n \in \mathbb{N}$ tal que $a^n = e$. Quano a tem ordem finita, o menor inteiro positivo m tal que $a^m = e$ chama-se ordem de a e é denotado por $o(a)$. Caso contrário, se não existir $n \in \mathbb{N}$ que satisfaça a propriedade, então a ordem de a é infinita.

Em um grupo, vale:

$$o(a) = 1 \Leftrightarrow a = e.$$

Exemplo 2.54. No grupo multiplicativo, $G = \{1, -1, i, -1\}$ temos que $o(-1) = 2$, pois $-i^2 = 1 = e$. Além disso, $o(i) = o(-i) = 4$.

Proposição 2.55. Seja G um grupo

1. Dado $a \in G$, $a \neq e$, temos $o(a) = 2 \Leftrightarrow a = a^{-1}$.
2. $o(a) = o(a^{-1})$, para todo $a \in G$.
3. Se $o(a) = 2$, para todo $a \in G - \{e\}$, então G é abeliano.
4. Se $o(a) = n \cdot m$, então $o(a^m) = n$.

Demonstração. 1. $\Rightarrow$) Se $o(a) = 2$, então $a^2 = e$. Como G é um grupo e possui elemento inverso, segue pela esquerda que

$$\begin{aligned} a^{-1} \cdot a^2 &= a^{-1} \cdot e \\ \Rightarrow a^{-1} \cdot a \cdot a &= a^{-1} \\ \Rightarrow a &= a^{-1}. \end{aligned}$$

Segue da mesma forma operando à direita do elemento em G.

$\Leftarrow$) Se $a = a^{-1}$, então $a^2 = e$. Isso implica que $o(a) = 2$, uma vez que $a \neq e$.

2. Suponha que $o(a) = n$. Então, $a^n = e$. Daí, temos

$$\begin{aligned} a^n = e \Leftrightarrow a^{-n} &= (a^n)^{-1} \\ &= e^{-1} \\ &= e. \end{aligned}$$

O menor elemento $m \in \mathbb{N}$ que satisfaz $a^m = e$ é também o menor que satisfaz a $(a^{-1})^n = e$. Logo, $o(a) = o(-a)$.

3. Por hipótese $o(a) = 2, \forall a \in G - \{e\}$. Pelo item (1), temos

$$a = a^{-1}, \forall a \in G.$$

Agora, dados $a, b \in G$, temos que $ab \in G$. Logo,

$$\begin{aligned} a \cdot b &= (a \cdot b)^{-1} \\ &= b^{-1} \cdot a^{-1}. \end{aligned}$$

Como todos os elementos têm a mesma ordem, então $a = a^{-1}$ e $b = b^{-1}$. Portanto,

$$a \cdot b = b \cdot a$$

e G é abeliano.

4. Por definição, se $o(a) = m \cdot n$, então $a^{m \cdot n} = e$, ou seja

$$(a^m)^n = e.$$

Resta provar que n é o menor inteiro positivo que satisfaz $(a^m)^n = e$. Tomando $r \in \mathbb{N}$, com $r < n$, tal que $(a^m)^r = e \Rightarrow a^{mr} = e$. Ou seja, $o(a) \leq m \cdot r$. Isso é um absurdo, pois $m \cdot r < m \cdot n$. Portanto, $o(a^m) = n$

□

Teorema 2.56. Sejam G um grupo e $a \in G$:

1. Se $a^n = e$, para algum $n \in \mathbb{Z}$, então $o(a)$ divide n.
2. Se $o(a) = m$, então para qualquer $k \in \mathbb{Z}$, $a^k = a^r$, sendo r o resto da divisão de k por m.

3. $o(a) = m$ se, e somente se, $< a >$ tem ordem m.

Demonstração. 1. Com $a^n = e$, considere $o(a) = m$. Daí, pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$, tais que

$$n = m \cdot q + r,\ 0 < r < m$$

Logo,

$$a^n = e \Rightarrow a^{m \cdot q + r} = e \Rightarrow (a^m)^q \cdot a^r = e \Rightarrow e^q \cdot a^r = e \Rightarrow a^r = e.$$

Portanto, pela minimalidade de m, $r = 0$ e $n = m \cdot q$.

2. Basta mostrar que, para cada $k \in \mathbb{Z}$, temos n$k = m \cdot q + r$, com $q, r \in \mathbb{Z}$ e $0 < r < m$. Daí, temos

$$\begin{aligned} e &= a^k \\ &= a^{m \cdot q + r} \\ &= (a^m)^q \cdot a^r \\ &= a^r. \end{aligned}$$

Como $a^k = e = a^r$, concluímos que $a^k = a^r$.

3. $\Rightarrow$) Se $o(a) = m$, isso significa que os elementos $e, a, a^2, a^3, \ldots, a^{m-1}$ são todos distintos. Supondo que $a^j = a^i$, para todo $0 < i < j < m - 1$, então $a^{j-i} = e$ e $j - i < m$. Absurdo, pois $o(a) = m$.

Ademais, considere $H = < a >$. Pelo item (2) temos $a^k = a^r$, com $k \in \mathbb{Z}$ e $r = \{0, 1, \ldots, m-1\}$. Daí, segue que $H = \{a^k; k \in \mathbb{Z}\} = \{a^r; r = 0, 1, \ldots, m-1\}$ tem ordem m.

$\Leftarrow$) Supondo que $H = < a >$ tem ordem finita, as potências de a^i, com $i \in \mathbb{Z}$, não podem ser todas distintas. Então, existem elementos que coincide, isto é, existem $i, j \in \mathbb{Z}$, tal que $a^i a^j$, com $i < j$. Ou seja, se $a^{j-i} = e$, então a ordem de a é finita, do tipo $o(a) = m$.

Contudo, no item anterior foi mencionado que os elementos $e, a, a^2, a^3, \ldots, a^{m-1}$ eram distintos. Dessa forma, pelo item (2), temos $< a > = \{a^r; r = 0, 1, \ldots, m-1\} = \{e, a, a^2, a^3, \ldots, a^{m-1}\}$. Portanto, a ordem de H é igual a m.

□

Corolário 2.57. Se G é um grupo finito, então existe $s \in \mathbb{N}$ tal que

$$a^s = e, \text{ para todo } a \in G.$$

Demonstração. Se G é um grupo finito, podemos escrevê-lo da seguinte forma

$$G = \{a_1, a_2, \ldots, a_k\}.$$

Pela observação 2.46, todo elemento de G tem ordem finita. Fazendo $o(a_i) = n \cdot i$, para $i \in \{1, \ldots, k\}$ e considerando s o produto dessas ordens $s = n_1 \cdot n_2 \ldots n_k$, tal que

$$a_i^s = \left(a_i^{n \cdot i}\right)^r = e, \forall a \in G,$$

em que $r = n_1 \cdot n_2 \ \cdot \ldots \cdot \ n_{i-1} \cdot n_{i+1} \cdot \ldots \cdot n_k$. □

3 TEOREMA DE LAGRANGE E APLICAÇÕES

3.1 Classe lateral

Ao trabalhar com grupos, uma questão importante que surge é como podemos entender as relações entre os elementos de um grupo e seus subgrupos. Em muitos casos, um subgrupo pode não ser suficiente para cobrir completamente o grupo, mas as operações que realizamos em torno desse subgrupo podem nos dar uma visão mais clara de como o grupo está estruturado.

Um exemplo interessante surge quando pensamos em aplicar a operação do grupo a um subgrupo. Se tomarmos um elemento qualquer g do grupo e o combinarmos com todos os elementos de um subgrupo H, formamos um conjunto de elementos que são chamados de "classe lateral" de H gerada por g. Intuitivamente, podemos pensar em uma classe lateral como uma "cópia deslocada" do subgrupo H, em que a operação de grupo é aplicada a partir de g.

O estudo das classes laterais nos permite entender melhor a "distribuição" dos elementos do grupo e como o grupo pode ser decomposto em subconjuntos que são estruturalmente semelhantes a um subgrupo, mas deslocados por um elemento específico. Esse conceito é central na teoria de grupos e é especialmente útil no entendimento das estruturas de grupos quocientes, que surgem a partir da divisão do grupo por um subgrupo.

Antes da definição de Classe Lateral, vejamos a seguinte proposição.

Proposição 3.1. Sejam G um grupo e H um subgrupo de G. Sobre G, vamos considerar a relação $\equiv_E (mod\ H)$, dada da seguinte maneira:

$$a \equiv_E b(mod\ H) \Leftrightarrow a^{-1}b \in H.$$

A relação $\equiv_E (mod\ H)$ é de equivalência.

Demonstração. Note que, para quaisquer x, y, z em G, tem-se:

1. Reflexiva: $x \equiv_E x(mod\ H)$, uma vez que $x^{-1}x = e \in H$. Logo, $\equiv_E$ é reflexiva.

2. Simétrica: Veja que:

$$\begin{aligned} x \equiv_E y(mod\ H) &\Rightarrow x^{-1}y \in H \\ &\Rightarrow (x^{-1}y)^{-1} \in H \\ &\Rightarrow y^{-1}x \in H \\ &\Rightarrow y \equiv_E x(mod\ H). \end{aligned}$$

Portanto, $\equiv_E$ é simétrica.

3. Transitiva: Note que, se $x \equiv_E y(mod\ H)$, e $y \equiv_E z(mod\ H)$, então xy^{-1}, $yz^{-1} \in H$. Desse modo, temos

$$\begin{aligned}(xy^{-1})(yz^{-1}) &\Rightarrow xz^{-1} \\ &\Rightarrow x \equiv_E z(mod\ H).\end{aligned}$$

Portanto, $\equiv_E$ é transitiva.

□

A classe de equivalência de um elemento $a \in G$, relativa a esta relação, é dada por $aH = \{\ ah : h \in H\}$ e é chamada de **classe lateral à esquerda de H em G determinada por** a. Analogamente definimos o conceito de classe lateral à direita de H em G determinda por a.

Sabendo que as classes à esquerda são uma relação de equivalência, então para todo $a \in G$,

$$G = \bigcup aH.$$

e para todo $x, y \in G$ temos $xH = yH$ ou $xH \cap yH = \varnothing$.

Definição 3.2. Sejam G um grupo e H um subgrupo de G. A cardinalidade do conjunto H_E (a mesma de H_D) chama-se **o índice** de H em G, o qual será indicado por $(G : H)$.

Exemplo 3.3. Com o grupo $G = (\ \mathbb{Z}_6, +)$ e subgrupo $H = \{\overline{0}, \overline{2}, \overline{4}\}$, as únicas classes laterais de H serão H e $\{\overline{1}, \overline{3}, \overline{5}\}$. Por este motivo, temos que $(G : H) = 2$.

Teorema 3.4. Sejam G um grupo e H um subgrupo de G, toda classe lateral à esquerda (à direita) tem a mesma cardinalidade de H. Ademais, os conjuntos H_E e H_D têm a mesma cardinalidade.

Demonstração. Tomando $g \in G$, considere a função

$$\begin{aligned}f : H &\to gH \\ h &\mapsto gh.\end{aligned}$$

Então, f é sobrejetiva. Além disso, dados $h_1, h_2 \in H$, temos, pela proposição 2.4,

$$\begin{aligned}f(h_1) = f(h_2) &\Rightarrow gh_1 = gh_2 \\ &\Rightarrow h_1 = h_2\end{aligned}$$

Assim, f é injetiva e, portanto, é bijetora. Segue o mesmo procedimento para

$$\begin{aligned}f : H &\to Hg \\ h &\mapsto hG\end{aligned}$$

Por outro lado,

$$\begin{aligned} \phi : H_E &\to H_D \\ gH &\mapsto Hg^{-1} \end{aligned}$$

é uma função de H_E em H_D. Daí, se g_1H e g_2H são elementos de H_E e $g_1H = g_2H$. Logo,

$$\begin{aligned} g_1 \equiv_E g_2 &\Leftrightarrow g^{-1}g_2 = h \in H \\ &\Leftrightarrow g^{-1} = hg_2^{-1}. \end{aligned}$$

Diante disso, temos

$$\begin{aligned} \phi(g_1H) = \phi(g_2H) &\Leftrightarrow Hg_1^{-1} = Hg_2^{-1} \\ &\Leftrightarrow g_1^{-1} \equiv_D g_2^{-1} \\ &\Leftrightarrow g_1^{-1}g_2 = h \in H \\ &\Leftrightarrow g_2 = g_1h. \end{aligned}$$

Daí, segue que

$$g_2H = g_1hH = g_1H$$

Portanto, ϕ é bijetora e, por isso, H_E e H_D têm a mesma cardinalidade. □

3.2 Teorema de Lagrange

O Teorema de Lagrange é um resultado central na teoria de grupos finitos e estabelece que, em um grupo finito, a ordem de qualquer subgrupo divide a ordem do grupo. Esse teorema revela uma importante relação entre a estrutura de um grupo e seus subgrupos, fornecendo uma ferramenta fundamental para a análise de grupos finitos. A demonstração desse teorema, que será apresentada a seguir, é uma das bases essenciais para o desenvolvimento da teoria dos grupos, oferecendo uma compreensão mais profunda da organização interna desses grupos.

Teorema 3.5. (Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então, a ordem de H divide a ordem de G. Em particular,

$$|G| = |H|.(G : H).$$

Demonstração. Sabendo que G é um grupo finito, seu índice também será finito. Suponha que $(G : H) = r$. Diante disso, vamos considerar que

$$H_E = \{a_1H, a_2H, \ldots, a_rH\}.$$

Como H_E é uma partição de G, temos

$$G = a_1H \dot{\cup} a_2H \dot{\cup} \ldots \dot{\cup} a_rH$$

Pelo Teorema 3.4, temos que a cardinalidade de cada classe em H_E é a mesma que a ordem de H. Logo, já que a união é disjunta,

$$|G| = |H| + |H| + |H| + \cdots + |H| = |H| \cdot r$$

Como $r = (G : H)$, concluímos que

$$|G| = |H| \cdot (G : H).$$

□

3.3 Aplicações

Aplicação 1: Sejam G um grupo finito e $g \in G$. Então, a ordem de g divide a ordem de G. Em particular,

$$g^{|G|} = e.$$

Demonstração. Pelo Teorema 2.56,

$$o(g) = |\langle g \rangle| .$$

Diante disso, aplicando o Teorema de Lagrange no subgrupo $\langle g \rangle$, temos que $o(g) := \lambda$ divide $|G|$. Então, existe $k \in \mathbb{N}$, tal que

$$|G| = \lambda.k.$$

Assim,

$$g^{|G|} = g^{\lambda.k} = (g^{\lambda})^k = e^k = e.$$

Portanto, a ordem de g divide a ordem de G. □

Aplicação 2: Todo grupo G de ordem prima é ciclico. Em particular, G é abeliano.

Demonstração. Considere $|G| = p$ primo e $a \in G$, com $a \neq e$. Daí, pelo Teorema de Lagrange,

$$|\langle g \rangle| \Big| |G|.$$

Então, $|\langle g \rangle| = 1$ ou $|\langle g \rangle| = p$. Porém, como $a \neq e$, segue que $|\langle g \rangle| = p$ e, assim, G é cíclico. Por conseguinte, G é abeliano. □

Aplicação 3: (Pequeno Teorema de Fermat): Sejam p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então,

$$a^{\,p-1} \equiv 1 (mod\ p).$$

Demonstração. Note que

$$U(\mathbb{Z}_p) = \{\bar{a} \in \mathbb{Z}_p \mid mdc(a,p) = 1\}.$$

Como p é primo, temos que

$$\mid U(\mathbb{Z}_p) \mid = p - 1.$$

Ora, mas como $p \nmid a$, então $\bar{a} \in U(\mathbb{Z}_p)$. Assim, da nossa primeira aplicação, segue que

$$\overline{a}^{p-1} = \overline{1} \Leftrightarrow \overline{a^{\,p-1}} \equiv \bar{1} \Leftrightarrow a^{p-1} \equiv 1\ (mod\ p).$$

□

Aplicação 4: Todo grupo G de ordem até cinco é abeliano.

Demonstração. Note que para os casos $|G| = 2$, $|G| = 3$ e $|G| = 5$ G é cíclico e abeliano, pois cada um deles têm ordem prima. Ademais, para $|G| = 1$, é imediato. Assim, o único caso que necessita de verificação é para $|G| = 4$.

Se existir $g \in G$ com $o(g) = 4$, então G é cíclico, concluindo assim o nosso resultado. Caso contrário, dado $g \neq e$, pelo Teorema 3.5 $o(g) = 2$. Como isso vale para todo $g \neq e$, segue do Teorema 2.56 o desejado. □

Aplicação 5: Seja G um grupo finito e sejam H e K subgrupos com ordem relativamente prima. Então $H \cap K = \{e\}$.

Demonstração. Pela Proposição 2.39, $H \cap K$ é um subgrupo de G e, portanto, também é de H e K. A partir disso, temos pelo Teorema 3.5 que

$$|H \cap K| \mid |H| \text{ e } |H \cap K| \mid |K|.$$

Como as ordens de H e K são relativamente prima, obtemos que $mdc(|H|,|K|) = 1$ e, consequentemente, $|H \cap K| = 1$. Portanto, $H \cap K = \{e\}$. □

Observação 3.6. Embora o Teorema de Lagrange seja válido para grupos finitos, sua recíproca não se mantém verdadeira. Em outras palavras, mesmo que a ordem de um subgrupo divida a ordem de um grupo, isso não implica necessariamente na existência de um subgrupo com essa ordem. Um contraexemplo clássico é o grupo alternado A_4, que é o grupo das permutações pares de quatro elementos. O grupo A_4 possui ordem 12, e seus subgrupos têm ordens 1, 2, 3, e 4. Embora a ordem 6 seja divisor de 12, não existe um

subgrupo de ordem 6 em A_4. Esse exemplo ilustra que a existência de divisores da ordem de um grupo não garante a existência de subgrupos correspondentes com essas ordens.

4 CONSIDERAÇÕES FINAIS

Neste trabalho, foi realizado o estudo da Teoria de Grupo, foram abordados os conceitos, propriedades e exemplos deste tópico para tratar de Grupos, Grupos abelianos, Subgrupos, Grupos clícicos, Grupos de permutação e Ordem de um grupo. Além disso, seguiu-se com a abordagem de Classes laterais, partindo para o Teorema de Lagrange e algumas aplicações. Ademais, após a discussão sobre o contraexemplo proporcionado pelo grupo A_4, é natural que surjam novas questões acerca da estrutura de grupos finitos e a existência de subgrupos com ordens específicas. Embora o Teorema de Lagrange forneça informações importantes sobre a ordem de subgrupos, ele não é suficiente para abordar questões mais complexas, como a contagem e a distribuição desses subgrupos. Para esses casos, os *Teoremas de Sylow* se mostram extremamente úteis, pois fornecem critérios precisos para a existência e o número de subgrupos de ordens determinadas. Ele afirma que dado um número inteiro primo e um grupo G, temos $|G| = p^m b$, com $mdc(p, b) = 1$. Então, para cada $0 \leq n \leq m$, existe um subgrupo H de G, com $|H| = p^n$. Contudo, uma análise mais profunda desse teorema está além do escopo deste trabalho, que se concentrou em uma introdução aos conceitos fundamentais da teoria de grupos e suas aplicações iniciais. Essas questões mais avançadas, relacionadas à estrutura interna dos grupos finitos, podem ser exploradas em trabalhos futuros.

REFERÊNCIAS

[1] DOMINGUES, Hygino; IEZZI, Gelson. **Álgebra Moderna**. 4.ed. [S.l.]: São Paulo, 2003.

[2] EVES, Howard. **Introdução à história da matemática**. 5.ed. São Paulo: Unicamp, 2011.

[3] FREITAS, Joel Gilvandro de. **O Teorema de Lagrange**. 55f. Trabalho de Conclusão de Curso (Graduação em Matemática). Universidade Estadual da Paraíba, Campina Grande, 2012.

[4] GONÇALVES, Adilson. **Introdução à Álgebra**. 5.ed. Rio de Janeiro. Editora SBM, 2015.

[5] PAIXÃO, Flaviane Panta. **Recíprocas do Teorema de Lagrange**. Trabalho de Conclusão de Curso (Graduação em Matemática). Instituto Federal da Bahia, Valença, 2023.

[6] SOUZA, Rodrigo Luiz de. **Uma Breve Introdução à Teoria de Grupos**. 73 f. Dissertação (Pós-Graduação) - Curso de Matemática, Universidade Federal de Santa Catarina. Florianópolis, 2014.

[7] VIEIRA, Vandenberg Lopes. **Álgebra abstrata para Licenciatura**. 1.ed. Campina Grande - PB: EDUEPB, 2013.

[8] XAVIER, Gustavo Santos. **Teorema de Lagrange: exemplos e aplicações da teoria de grupos**. 43 f. TCC (Graduação) - Curso de Matemática, Universidade Federal do Tocantins, Araguaína, 2022.